УДК 004.4

ЭЛЕКТРОННАЯ ПОДПИСЬ - ОБУЧАЮЩИЕ И ТЕСТИРУЮЩИЕ КОМПЛЕКСЫ

А.А. Большакова[1]

1 *anastaicha94@mail.ru*; Кубанский государственный университет, г. Краснодар

Описаны алгоритмы формирования и проверки электронной подписи по ГОСТ Р 34.10-2012 и по алгоритму RSA в Microsoft Visual Studio 2012.

Ключевые слова: электронная подпись, асимметричные схемы, открытый ключ, закрытый ключ, хэш-функция, хэш-код, криптостойкость.

Под ЭП понимают реквизит электронного документа, который предназначен для его защиты от подделок. Реквизит получают в итоге криптографического преобразования информации с закрытым ключом. Также подпись позволяет идентифицировать владельца сертификата ключа подписи и установить отсутствие искажения информации в электронном документе.

Согласно Федеральному закону от 06.04.2011 № 63-ФЗ «Об электронной подписи» использование ЭП возможно исключительно для электронных и никаких других документов.

ГОСТ Р 34.10-2012 определяет схему электронной подписи, процессы формирования и проверки подписи под заданным сообщением (документом), передаваемым по незащищенным телекоммуникационным каналам общего пользования в системах обработки информации различного назначения. Внедрение подписи на основе вышеуказанного стандарта повышает, по сравнению с ранее действовавшей схемой цифровой подписи, уровень защищенности передаваемых сообщений от подделок и искажений. Областью применения стандарта является создание, эксплуатация и модернизация систем обработки информации различного назначения.

Обязательными идентификационными реквизитами электронного документа являются:

1) наименование и обозначение электронного документа;

2) даты создания, утверждения и последнего изменения;

3) сведения о создателях;

4) сведения о защите электронного документа;

5) сведения о средствах ЭП или средствах кэширования, необходимых для проверки подписи или контрольной характеристики данного электронного документа;

6) сведения о технических и программных средствах, необходимых для воспроизведения электронного документа;

7) сведения о составе электронного документа.

Электронная подпись позволяет осуществить переход от бумажных носителей информации к электронному документообороту. Более того, ЭП предназначена для подтверждения авторства, иными словами для идентификации лица, подписавшего электронный документ, так как фактически является аналогом собственноручной подписи.

С помощью ЭП осуществляются следующие функции:

1) контроль целостности передаваемого документа: если документ с ЭП претерпит изменения случайные или преднамеренные, ЭП автоматически станет недей-

ствительной в связи с тем, что вычислена она на основании первоначального документа и соответствует только ему;

2) защита от изменений, фактически подделки, электронного документа: ЭП гарантирует выявление подделок с помощью контроля целостности, что делает подделывание бессмысленным за исключением частных случаев;

3) невозможность отказа от авторства: создание исправной подписи требует знания закрытого ключа, который находится у владельца ЭП. Следовательно, наличие подписи под документом гарантирует авторство владельца ЭП;

4) доказательственное подтверждение авторства электронного документа: создание исправной подписи возможно лишь с помощью закрытого ключа, который находится у владельца. Так, при необходимости подтверждения владельцем подписи электронного документа, такому лицу достаточно предъявить открытый и закрытый ключи. В соответствии с особенностями документа подписываются различные поля. Например: автор, изменения, время и прочее.

Таким образом, ЭП используют в следующих целях:

1) банковские системы;

2) электронная торговля;

3) государственные закупки;

4) таможенные декларации;

5) регистрация сделок с недвижимостью;

6) контроль исполнения государственного бюджета;

7) контроль исполнения лимитов бюджетных обязательств и выделенных субсидий;

8) обращение к органам власти через электронные системы;

9) обязательная отчетность перед государственными учреждениями и внебюджетными фондами;

10) организация юридически весомого электронного документооборота;

11) в трейдинговых и расчетных системах;

12) межбанковского рынка обмена валют в глобальных системах;

13)управление акционерным капиталом и долевым участием.

Учитывая огромное влияние ЭП на документооборот в целом и широчайший диапазон областей её применения в частности, невозможно не заинтересоваться столь актуальным вопросом, а именно изучением и тестированием подписи.

Алгоритмы шифрования электронной подписи делятся на несколько типов: симметричные, ассиметричные и комбинированные.

Асимметричные схемы ЭП — криптосистема с открытым ключом. Асимметричное шифрование производится с помощью открытого, а дешифрование — с помощью закрытого ключей, в ассиметричных алгоритмах электронной подписи подписание производится с закрытого, а проверка подписи — с открытого ключей.

Общепринятая схема цифровой подписи объединяет три процесса *(Gen, Sign, Vrfy)*:

1) генерация пары ключей Gen равновероятным образом, из возможных закрытых ключей выбирается закрытый ключ *sk*, вычисляется соответствующий открытый ключ *pk*, где $|pk| \geq n$, 1^n — секретный параметр. На выходе: $(pk; sk; s_0)$;

2) алгоритм подписи Sign для заданного электронного документа M с помощью

закрытого ключа *sk* и величины s_{i-1} вычисляется подпись ζ с величиной s_i: $(\zeta, s_i) \leftarrow Sign_{sk,s_{i-1}}(m)$;

3) проверка подписи *Vrfy* для данных документа M и подписи ζ с помощью открытого ключа *pk* определяется действительность подписи как $b := Vrfy_{pk}(M,\zeta)$ бит.

Применение ЭП имеет смысл, если:

1) верификация подписи производится открытым ключом, соответствующим закрытому, применяемому при подписании электронного документа;

2) отсутствие закрытого ключа влечет за собой вычислительно сложный процесс формирования легитимной подписи.

Обеспечение второго пункта в асимметричных алгоритмах ЭП опирается на ряд вычислительных задач:

1) задача дискретного логарифмирования (EGSA);

2) задача факторизации (RSA).

Стоит заметить, что при одинаковой длине ключа (например 1300 бит) криптостойкости алгоритмов RSA и ElGamal равны $(2,7 \cdot 10^{28})$, а вот у алгоритма ECDSA скорость и криптостойкость работы выше.

Существуют два основных способа вычисления: на базе математического аппарата эллиптических кривых (ГОСТ Р 34.10-2012) и на базе полей Галуа (DSA). На данный момент субэкспоненциальные алгоритмы являются самыми быстрыми алгоритмами дискретного логарифмирования и факторизации.

Алгоритм формирования и проверки подписи соответственно по ГОСТ Р 34.10-2012 опишем следующим образом:

Для того чтобы цифровая подпись была сформирована под сообщение M приводится следующий алгоритм:

1) вычисляем хэш-кода от сообщения M: $\overline{h} = h(M)$;

2) вычисляем $\alpha \in Z$ (соответствующего $\bar{h}$) и определяем $e = \alpha \bmod q$, в случае, когда $e = 0$, заменяем на $e = 1$;

3) генерация случайного (псевдослучайного) $k \in Z : 0 < k < q$;

4) вычисление точки эллиптической кривой $C = k \cdot P$, $r = x_c \bmod q$, где x_c — координата x точки C. Если $r = 0$, возвращаемся к генерации;

5) вычисление $s = (rd + ke) \bmod q$, если $s = 0$, возвращаемся к генерации;

6) конкатенацией $\bar{r}$ и $\bar{s}$, с соответствующими r и s, формируем цифровую подпись: $\zeta = \left(\overline{r} || \overline{s}\right)$.

Для проверки подписи приводится следующий алгоритм:

1) вычисляем числа r и s по ζ. Если $0 < r < q$ и $0 < s < q$ выполнены, идем дальше, в противном случае подпись неверна;

2) вычисляем хэш-код сообщения M: $\overline{h} = h(M)$;

3) вычисляем $\alpha \in Z$ (соответствующего $\overline{h}$) и определяем $e = \alpha \bmod q$, в случае, когда $e = 0$, заменяем на $e = 1$;

4) вычисляем $v = e^{-1} \bmod q$;

5) вычисляем $z_1 = sv \bmod q$ и $z_2 = -rv \bmod q$;

6) вычисляем точку эллиптической кривой $C = z_1 P + z_2 Q$ и $R = x_c \bmod q$, где x_c — координата x точки C;

7) если $R = r$ подпись подтверждена, если $R \neq r$ — не подтверждена.

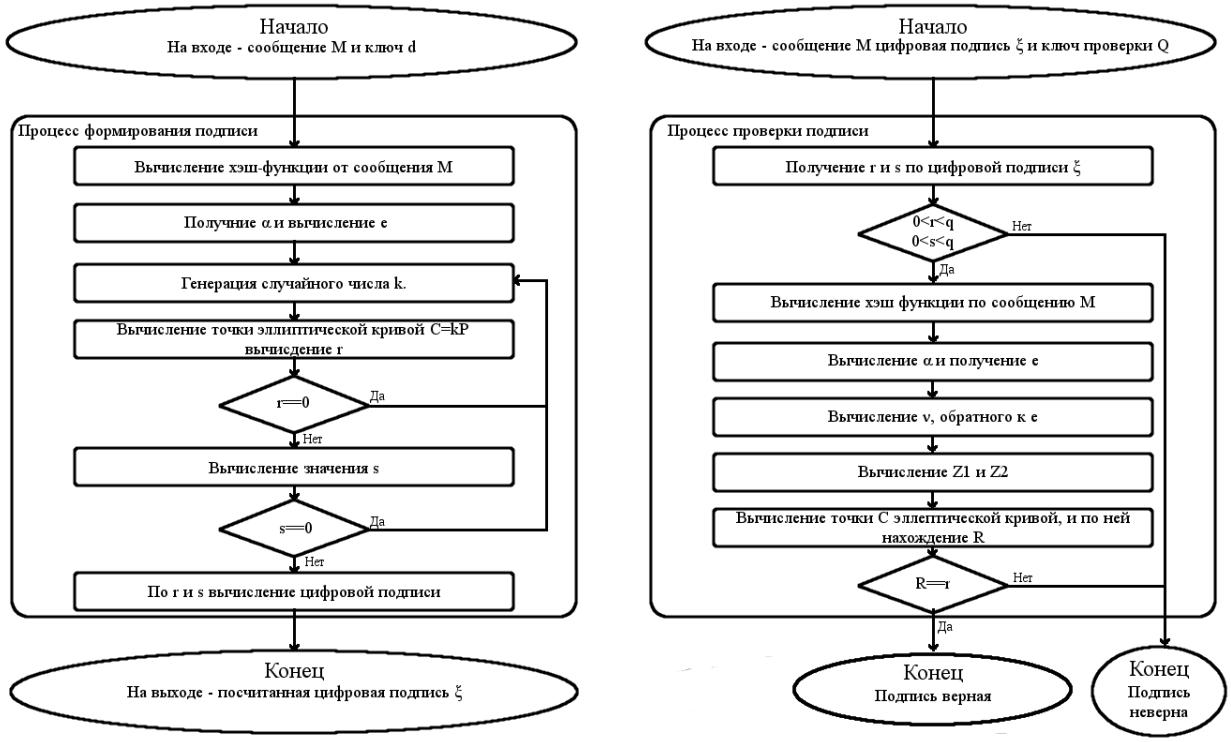

Рис. 1. Формирование и проверка цифровой подписи

Реализуем ЭП на основе алгоритма RSA с хэш-функцией MD5 в среде разработки Microsoft Visual Studio 2012 на языке программирования — C++.

Входными данными служит текстовое сообщение, которое открывается из файла формата .txt. Текст сообщения может содержать латинский алфавит, различные символы и цифры. На выходе программа предоставляет информацию о значениях простых чисел p и q, открытого и закрытого ключей, цифровую подпись, хэш-код функции MD5 и статус подтверждения подлинности цифровой подписи, выдаваемый отдельным запросом.

В программе реализованы следующие процессы:

1) ввод данных непосредственно из текстового файла;

2) возможность получения дополнительной информации о программе;

3) возможность запуска цифровой подписи с автоматической генерацией;

4) вывод результатов работы программы во всплывающем окне и в самой форме.

Алгоритм программа разработан на основе алгоритма RSA с функцией хэширования MD5.

Генерация ключей:

1) генерируются два простых отличных друг от друга числа p и q;

2) вычисляется модуль $n = p \cdot q$;

3) вычисляется функция Эйлера от модуля $\phi(n) = (p-1)(q-1)$;

4) выбирается открытая экспонента e: $\begin{cases} 1 < e < \phi(n) \\ (e, \phi(n)) = 1 \end{cases}$;

5) вычисляется закрытая экспонента d: $d \equiv e^{-1} \bmod \phi(n) \Rightarrow de \equiv 1 \bmod \phi(n)$;

6) пара чисел (e, n) образуют открытый ключ;

7) пара чисел (d, n) образуют закрытый ключ.

Алгоритм подписи:

1) m — сообщение;

2) с помощью алгоритма хэш-функции MD5 из сообщения m получается хэш-код: $h = H(m)$;

3) формируется подпись: $sign = h^d \bmod n$;

4) передается сообщение с ЭП $(m, sign)$.

Проверка подписи:

1) принимается сообщение с ЭП $(m, sign)$;

2) вычисляется хэш исходного сообщения: $h = sign^e \bmod n$;

3) вычисляется хэш пришедшего сообщения $H(m)$;

4) проверяется равенство $h = H(m)$, если равенство подтвердилось, подпись верна, иначе — не верна.

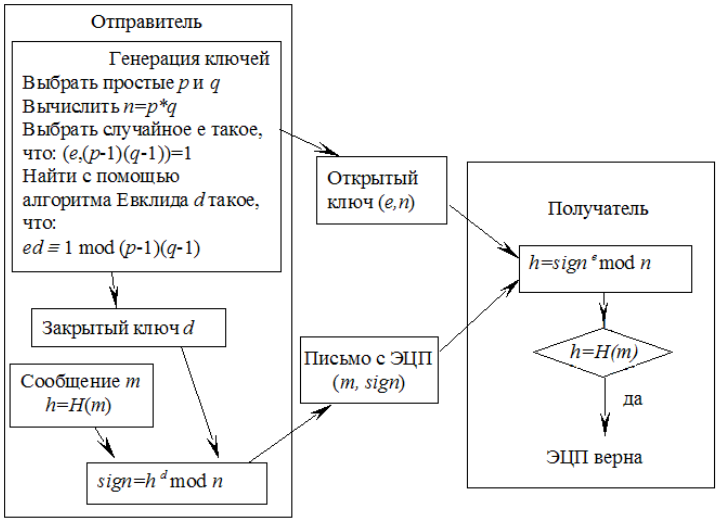

Рис. 2. Алгоритм ЭП на основе RSA

Алгоритм хэш-функции MD5, применяемый для реализации данной программы, основан на статье Рональда Ривеста.

Для удобства анализа ЭП было создано графическое окно. Управление компонентами программы реализуется с помощью мыши.

Меню программы состоит из следующих компонентов:

1) файл;

2) о программе;

3) кнопки: свернуть, развернуть, выход.

В пункте «Файл» имеется подпункт «Открыть», он считывает и выводит содержимое текстового файла в окне, под надписью «*Содержимое файла:* ». Окно содержит полосу прокрутки. Если по каким-то причинам файл открыть не удалось, нам сообщат об этом с помощью всплывающего окна. Также, в этом окне присутствует кнопка «ОК» и красная кнопка закрытия. Нажатие на любую из них приведет нас обратно на главную форму.

При выборе пункта «О программе» появляется всплывающее окно, в котором содержится некоторая информация об авторе программы: ФИО, группа, факультет. Также, в этом окне присутствует кнопка «ОК» и красная кнопка закрытия. Нажатие на любую из них приведет нас обратно на главную форму.

Кнопки: свернуть, развернуть, выход используются по прямым назначениям.

На самой форме присутствуют еще две кнопки:

1) Запустить цифровую подпись с автоматической генерацией;

2) Проверка цифровой подписи.

При первоначальной загрузке формы отключаются кнопки запуска алгоритма. Они активизируются только после удачного открытия, считывания и отображения текстового файла в соответствующий textbox.

При активизации первой кнопки заполняются все поля формы:

1.1) «*P* =» ;

1.2) «*Q* =» ;

1.3) *Открытый ключ:* ;

1.4) *Закрытый ключ:* ;

1.5) окно под надписью «*Цифровая подпись через RSA*»;

1.6) *MD5 хэш-код:* .

В первом и во втором пунктах выводятся большие простые числа. Третий и четвертый пункты вычисляются алгоритмом, их невозможно выделить и (или) скопировать. В пятом — цифровая подпись. Шестой пункт также нельзя ни выделить, ни скопировать, содержащийся в строке хэш-код хэш-функции MD5.

Активизация кнопки «Проверка цифровой подписи» вызывает всплывающее окно, которое содержит информацию либо о подтверждении, либо о не подтверждении цифровой подписи. Также, в этом окне присутствует кнопка «OK» и красная кнопка закрытия. Нажатие на любую из них приведет нас обратно на главную форму.

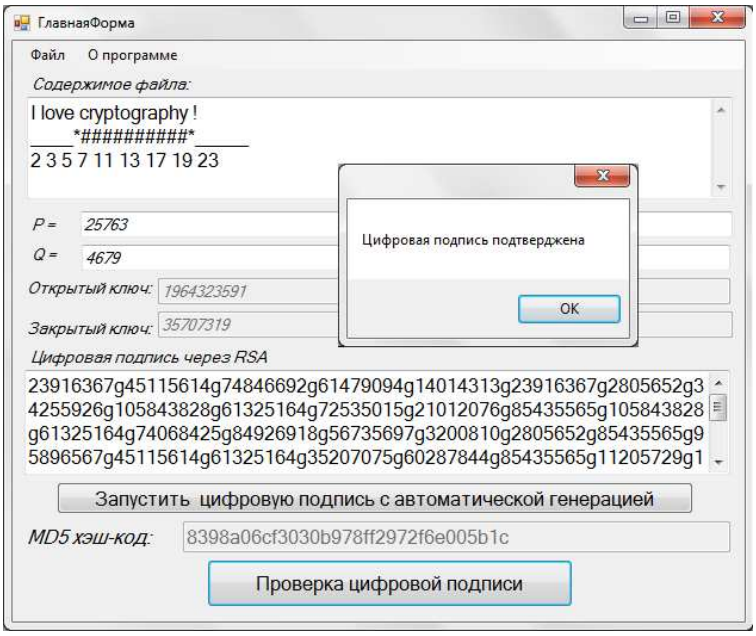

Рис. 3. Проверка ЭП

Рассмотрим работу программы на тестовых примерах. После открытия текстового файла и считывания данных из него на окно, запускаем автоматическую генерацию цифровой подписи, нажатием на соответствующую кнопку и проверяем ЭП.

При повторной генерации обновляются все поля, кроме хэш-кода и окна с тек-

стом файла. Чтобы значения функции хэширования изменились, откроем новый текстовый файл, считаем его и еще раз запустим генерацию. Как и прежде, проверка цифровой подписи выдает положительный результат:

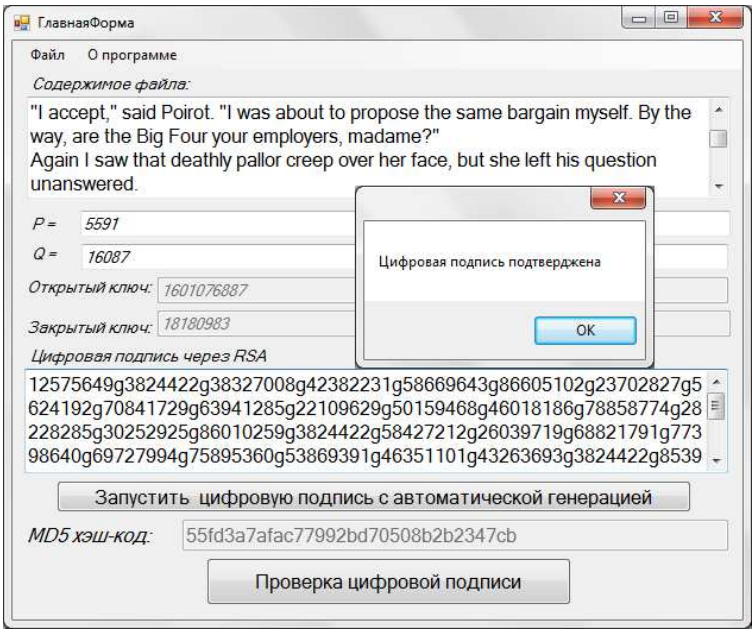

Рис. 4. Проверка нового текстового файла

Чтобы цифровая подпись перестала подтверждаться, нужно изменить содержимое файла, отображаемое в окне формы. Для этого достаточно изменить хотя бы один символ текста:

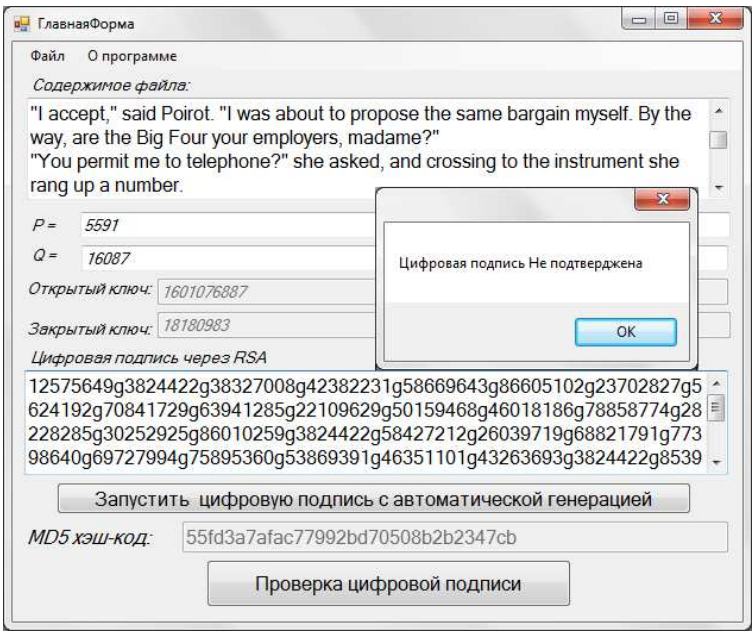

Рис. 5. Проверка ЭП

Через ЭП в мире проходят сделки примерно на 15 % мирового ВВП — это 10 триллионов долларов в год. Электронная подпись обеспечивает и безбумажный документооборот, что составляет миллиарды документов в день.

Благодаря ЭП, находясь у себя дома или в офисе, стало возможным подписывать различные документы, участвовать в электронных торгах, заказать какой-либо до-

кумент и многое другое в любой точке земного шара.

Более того, уже сейчас стало возможным заказать и получить ЭП дистанционно.

ЭП используется и в универсальных электронных картах. Стоит заметить, что с 01.01.2013 гражданам РФ выдаётся УЭК, в которую встроена КЭП.

Перспективы — это применение схем ЭП на SIM-картах.

Математическая проблема в том, что нет математических методов проверки корректности работы хэш-функции и самой ЭП. Именно поэтому во всем мире используется по сути одни и те же алгоритмы: схема Эль Гамаля, плюс не криптографический хэш Рона Ривеста (RSA).

Литература

1. Об электронной подписи: Федеральный закон от 06.04.2011 № 63-ФЗ // Собрание законодательства. - 2011.

2. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Введен в действие Приказом Росстандарта от 07.08.2012 № 215-ст.

3. Rivest R. The MD5 Message-Digest Algorithm / R. Rivest // Network Working Group.-1992.- Access mode: http://md5x.ru/images/rfc/rfc1321.txt.

4. McAndrew A. Introduction to Cryptography with Open-Source Software / A. McAndrew. - CRC Press, 2011.

ELECTRONIC SIGNATURE — SOFTWARE SYSTEMS FOR TRAINING AND TESTING

A.A. Bolshakova

The algorithms of generation and verification electronic signature in accordance with GOST R 34.10-2012 and the RSA algorithm in the Microsoft Visual Studio 2012.

Keywords: electronic signature, asymmetrical scheme, public key, private key, hash function, hash-code, cryptographic.

УДК 539.3

ИСПОЛЬЗОВАНИЕ СИСТЕМЫ MAPLE ДЛЯ ПОСТРОЕНИЯ ФУНКЦИИ ГРИНА ПРЯМОУГОЛЬНОЙ ПЛАСТИНЫ

Д.П. Голоскоков[1]

1 *goloskokovdp@gumrf.ru*; Государственный университет морского и речного флота имени адмирала С.О. Макарова, г. Санкт-Петербург

Описан алгоритм построения функции Грина для прямоугольной пластины в СКМ Maple.

Ключевые слова: компьютерное моделирование, пластина, функция Грина.

Рассматривается краевая задача в области $\Omega = \{(x, y) : 0 \le x \le 1, 0 \le y \le 1\}$, описываемая дифференциальным уравнением в безразмерной форме